PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :
G05B 19/042, G06F 11/00

A1

(11) Internationale Veröffentlichungsnummer: **WO 99/36840**

(43) Internationales Veröffentlichungsdatum: 22. Juli 1999 (22.07.99)

(21) Internationales Aktenzeichen: PCT/DE98/03771

(22) Internationales Anmeldedatum: 22. Dezember 1998 (22.12.98)

(30) Prioritätsdaten:
198 01 137.7 14. Januar 1998 (14.01.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: TRAUTH, Armin [DE/DE]; Lindenstrasse 40, D–76829 Landau (DE). ZÄCH, Jörg–Peter [DE/DE]; Hallstädterweg 44, D–90425 Nürnberg (DE). WEBER, Karl [DE/DE]; Zur Schanze 5, D–90518 Altdorf (DE). BIRZER, Johannes [DE/DE]; Dr.–Ram–Strasse 8, D–92536 Pfreind (DE). BARTHEL, Herbert [DE/DE]; Am Hasengarten 6A, D–91074 Herzogenaurach (DE). SCHÜTZ, Hartmut [DE/DE]; Friedhofstrasse 6, D–91336 Heroldsbach (DE). FUCHS, Heiner [DE/DE]; Wolfstaudenring 13 A, D–91056 Erlangen (DE). VON KROSIGK, Hartmut [DE/DE]; Platanenweg 3, D–91058 Erlangen (DE). SCHENK, Andreas [DE/DE]; Schenkstrasse 82, D–91052 Erlangen (DE).

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D–80506 München (DE).

(81) Bestimmungsstaaten: CN, ID, JP, KR, SG, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

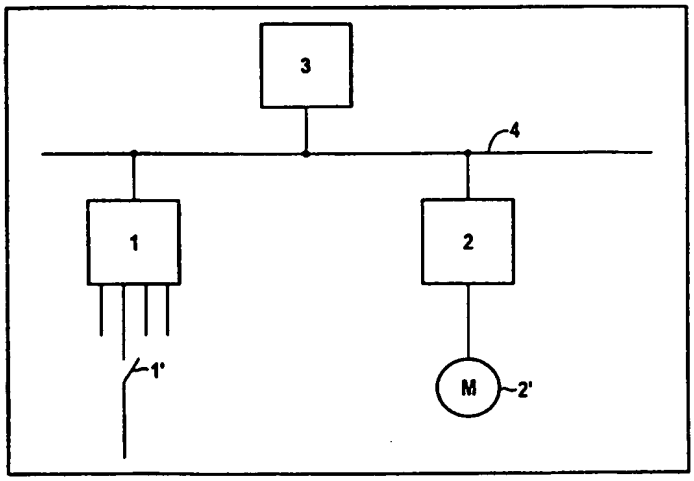
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: TROUBLEPROOF PROCESS INPUT AND OUTPUT

(54) Bezeichnung: FEHLERSICHERE PROZESSEINGABE UND PROZESSAUSGABE

(57) Abstract

Disclosed is a method for operating an automation system, whereby the automation system has at least one input unit to receive process signals, at least one output unit controlling an external peripheral device and both units are connected to each other for communication purposes by means of a bus. The inventive method is characterised in that at least one of the input units and at least one of the output units are embodied as a troubleproof input unit (EE) or a troubleproof output unit (AE). The inventive method is also characterised in that the troubleproof input unit (EE) transfers a telegram to the troubleproof output unit (AE) at given moments in time and that the telegram (T) contains at least one item of useful information, one destination point code (TT) designating the addressed output unit (AE) and one origin code (TS) designating the transmitting input unit (EE). The invention is further characterized in that the output unit (AE) evaluates continual reception of the telegram (T) as an indication of an intact communication relation and shifts the connected peripheral device into a safe state.



(57) Zusammenfassung

Es wird ein Verfahren zum Betrieb eines Automatisierungssystems angegeben, wobei das Automatisierungssystem mindestens eine Eingabeeinheit zur Aufnahme von Prozeßsignalen und mindestens eine Ausgabeeinheit zum Ansteueren externer Peripherie aufweist, die kommunikativ über einen Bus miteinander verbunden sind, wobei sich das Verfahren dadurch auszeichnet, daß zumindest eine der Eingabeeinheiten und zumindest eine der Ausgabeeinheiten als fehlersichere Eingabeeinheit (EE) bzw. fehlersichere Ausgabeeinheit (AE) ausgebildet sind, und daß die fehlersichere Eingabeeinheit (EE) der fehlersicheren Ausgabeeinheit (AE) zu vorgegebenen Zeitpunkten ein Telegramm (T) übermittelt, und daß das Telegramm (T) zumindest eine Nutzinformation (TN), eine die adressierte Ausgabeeinheit (AE) bezeichnende Zielkennung (TT) und eine die sendende Eingabeeinheit (EE) bezeichnende Ursprungskennung (TS) aufweist, und daß die Ausgabeeinheit (AE) den kontinuierlichen Empfang des Telegramms (T) als Indiz für eine intakte Kommunikationsbeziehung auswertet und andernfalls die angeschlossene Peripherie in einen sicheren Zustand überführt.

Beschreibung

Fehlersichere Prozeßeingabe und Prozeßausgabe

Die vorliegende Erfindung betrifft ein Verfahren zum Betrieb eines Automatisierungssystems, wobei das Automatisierungssystem mindestens eine Eingabeeinheit zur Aufnahme von Prozeßsignalen und mindestens eine Ausgabeeinheit zum Ansteuern externer Peripherie aufweist, wobei die Eingabeeinheit und die Ausgabeeinheit kommunikativ über einen Bus miteinander verbunden sind.

Um bei Automatisierungsvorhaben, die von einem gattungsgemäßen Automatisierungssystem gesteuert und/oder überwacht werden, in Notsituationen ein schnelles Abschalten der automatisierten Prozesse oder einzelner Vorgängen zur erreichen, ist bisher eine Not-Aus-Behandlung in Form einer Not-Aus-Kette vorgesehen.

In eine derartige Not-Aus-Kette werden Not-Aus-Schalter, Lichtgitter, Tretmatten oder Ähnliches integriert. Aufgrund der an eine Not-Aus-Behandlung zu stellenden Anforderungen ist es üblich, die Not-Aus-Behandlung in herkömmlicher Verdrahtung auszuführen. Als Beispiel sei hier ein Tunnelofen genannt, der bezüglich des Automatisierungsprozesses in mehrere Segmente unterteilt ist. An für den Benutzer zugänglichen Positionen an der Außenseite des Tunnelofens sind für die Not-Aus-Behandlung z.B. Not-Aus-Taster vorgesehen, wobei die Betätigung eines Not-Aus-Tasters je nach Auslegung der automatisierten Gesamtanlage, z.B. das definierte Herunterfahren des gesamten Prozesses nach sich zieht.

Die Not-Aus-Taster sind Feldgeräte mit einer Eingabefunktion. Die Geräte, die das Herunterfahren des Prozesses bewirken, sind entsprechend Geräte mit einer Ausgabefunktion zur An-

steuerung externer Peripherie, z.B. also Ausgabegeräte, die einen Motor für Transportprozesse, einen Motor für Ventilation, ein Hydraulikaggregat zur Positionierung o.ä. steuern.

Im Falle einer Not-Aus-Situation ist das unmittelbare Abschalten der externen Peripherie erforderlich. Zu diesem Zweck ist zwischen den Eingabegeräten, also den Not-Aus-Tastern, und den Ausgabegeräten, wie den Motoren oder den Aggregaten, eine Not-Aus-Kette aufgebaut, die bisher in konventioneller Verdrahtung auszuführen war und die beim Betätigen eines Not-Aus-Tasters ein unmittelbares Abschalten des Motors bzw. ein unmittelbares Abschalten des Hydraulikaggregates bewirkt. Die konventionelle Verdrahtung ist dabei bisher aufgrund der Sicherheitsanforderungen, die an eine Not-Aus-Behandlung zu stellen sind, erforderlich.

Dabei ist es jedoch nachteilig, bei großflächigen Automatisierungsprojekten wie z.B. bei den beschriebenen Tunnelöfen, die konventionelle Verdrahtung im gesamten Prozeßfeld vorzusehen.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren zum Betrieb eines Automatisierungssystems anzugeben, bei dem zur Behandlung von Not-Aus-Situationen auf die konventionelle Verdrahtung verzichtet werden kann und statt dessen eine kommunikative Verbindung zwischen den Komponenten der Not-Aus-Kette über den Bus des Automatisierungssystems besteht.

Erfindungsgemäß ist daher vorgesehen, für die Not-Aus-Behandlung auf die konventionelle Verdrahtung zu verzichten und sämtliche Feldgeräte, d.h. also auch die Not-Aus-Taster und die in die Not-Aus-Kette einzubindenden Motoren oder Aggregate, über den Prozeßbus kommunikativ zu verbinden.

Diese Aufgabe wird für ein Verfahren zum Betrieb eines Automatisierungssystems, wobei das Automatisierungssystem mindestens eine Eingabeeinheit zur Aufnahme von Prozeßsignalen und mindestens eine Ausgabeeinheit zum Ansteuern externer Peripherie aufweist, wobei die mindestens eine Eingabeeinheit und die mindestens eine Ausgabeeinheit kommunikativ über einen Bus miteinander verbunden sind, dadurch gelöst, daß zumindest eine der Eingabeeinheiten und zumindest eine der Ausgabeeinheiten als fehlersichere Eingabeeinheit bzw. fehlersichere Ausgabeeinheit ausgebildet sind, daß die fehlersichere Eingabeeinheit der fehlersicheren Ausgabeeinheit zu vorgegebenen Zeitpunkten ein Datum übermittelt, daß das Datum zumindest ein Nutzinformation, eine die adressierte Ausgabeeinheit bezeichnende Zielkennung und eine die sendende Eingabeeinheit bezeichnende Ursprungskennung aufweist, daß die Ausgabeeinheit den kontinuierlichen Empfang des Datums als Indiz für eine intakte Kommunikationsbeziehung auswertet und andernfalls die angeschlossene Peripherie in einen sicheren Zustand überführt.

Die an eine Not-Aus-Behandlung zu stellenden Sicherheitsanforderungen werden gemäß der Erfindung erfüllt, wenn die Eingabegeräte, also z.B. die Not-Aus-Taster und die in die Not-Aus-Kette einzubindenden Ausgabegeräte, die zur Ansteuerung der Motoren oder Aggregate vorgesehen sind, jeweils fehlersicher ausgeführt sind. Im Falle einer Not-Aus-Situation ergibt sich dann in der automatisierten Anlage folgender Ablauf:

Beim Betätigen eines Not-Aus-Tasters wird durch das Dateneingabegerät ein Datum auf den Bus gelegt. Das zu übermittelnde Datum weist gemäß den Spezifikationen des für die physikalische Kommunikationsverbindung verwendeten Busprotokolls zumindest ein Nutzinformation, in diesem Falle also die Information, ob der Not-Aus-Taster gedrückt ist oder nicht, zumindest eine Zieladresse, also die Adresse des Kommunikation-

steilnehmers, an die die Nachricht gesendet wird - wobei eine spezielle Kennung ein Versenden der Nachricht an alle Kommunikationsteilnehmer ermöglicht - sowie schließlich die Ursprungskennung, die den Absender des Datums identifiziert, auf.

Die Erfindung kann nun einmal so eingesetzt werden, daß das Datum an einen ganz bestimmten Kommunikationsteilnehmer versendet wird, wobei der Adressat anhand der im Datum enthaltenen Zieladresse erkennt, daß das Datum für ihn bestimmt ist, oder daß das Datum an alle Kommunikationteilnehmer versendet wird, wobei jeder einzelne Kommunikationsteilnehmer anhand der Ursprungsadresse des Datums ermittelt, ob das Datum, also die Nutzinformation des Datums von ihm auszuwerten ist.

Andererseits kann das Datum auch an eine übergeordnete Einheit des Automatisierungssystems, z.B. die Zentraleinheit einer speicherprogrammierbaren Steuerung, versendet werden, wobei diese wiederum an der Ursprungskennung des Datums erkennt, daß eine Nachricht, z.B. von einem Not-Aus-Taster eingetroffen ist, die einer unmittelbaren Behandlung bedarf, so daß die Zentraleinheit unmittelbar nach Detektion des Datums dieses an die Ausgabegeräte weiterleitet, so daß diese ein Herunterfahren bzw. Abschalten der an die Ausgabegeräte angeschlossenen Motoren oder Aggregate auslösen bzw. selbst ein weiteres Datum an die Ausgabegeräte absetzen, das zum gleichen Resultat führt.

Die Ausgabeeinheit wertet dabei den kontinuierlichen Empfang des Datums von der Eingabeeinheit als Indiz für eine intakte Kommunikationsbeziehung. Für den Fall, daß die Ausgabeeinheit das Ausbleiben eines Datums von einer Eingabeeinheit während einer Zeitspanne, die größer als eine vorgebbare Zeitspanne ist, feststellt, überführt die Ausgabeeinheit die angeschlossene Peripherie in einem sicheren Zustand und sorgt damit

wieder für das Herunterfahren der angeschlossenen Motoren oder Aggregate.

Zum Einsatz im Rahmen des erfindungsgemäßen Verfahrens zum Betrieb eines Automatisierungssystems ist ferner ein fehlersicheres Dateneingabegerät mit mindestens einem Eingabekanal zum Anschluß peripherer Sensorik vorgesehen, für das eine Prüfschaltung vorgesehen ist, die zu vorgegebenen Zeiten einen Prüfvorgang auslöst und dabei für mindestens einen der Eingabekanäle des fehlersicheren Eingabegerätes einen Statuswechsel bewirkt, wobei eine interne Logik den Statuswechsel überwacht und ggfs. eine Fehlermeldung ausgibt, wobei der durch die Prüfschaltung bewirkte Statuswechsel am Ende des Prüfvorgangs wieder rückgängig gemacht wird und wobei der Prüfvorgang für das Auslesen des betroffenen Eingabekanals vollkommen transparent ist.

Für den Einsatz im Rahmen des erfindungsgemäßen Verfahrens zum Betrieb eines Automatisierungssystems ist ferner oder alternativ ein fehlersicheres Dateneingabegerät mit mindestens einem Eingabekanal zum Anschluß peripherer Sensorik vorgesehen, bei dem der mindestens eine Eingabekanal antivalent ausgelegt ist.

Die gemäß der obenstehenden Beschreibung ausgeführten fehlersicheren Eingabegeräte werden durch die genannten Maßnahmen, d.h. durch die antivalente Auslegung des Eingabekanals bzw. durch die Überwachung des Eingabekanals mittels einer Prüfschaltung zu fehlersicheren Dateneingabegeräten, wobei die beiden Maßnahmen auch kombinierbar sind.

Zum Einsatz im Rahmen des erfindungsgemäßen Verfahrens zum Betrieb eines Automatisierungssystems ist ferner eine fehlersicheres Ausgabegerät ausgebildete Ausgabeeinheit vorgesehen.

Wenn für das fehlersichere Datenausgabegerät eine Verarbeitungseinheit zur Verarbeitung benutzer-projektierbarer logischer Verknüpfungen vorgesehen ist, wobei die Verarbeitungseinheit das Nutzinformation eines empfangenen Datums auswertet, das Nutzinformation der benutzerprojektierbaren logischen Verknüpfung unterwirft und entsprechend dem Ergebnis der logischen Verknüpfung den mindestens einen Ausgabekanal ansteuert, sind Softwarekomponenten, die bisher üblicherweise in einem übergeordneten Automatisierungsgerät, z.B. der Zentraleinheit einer speicherprogrammierbaren Steuerung, vorgesehen waren, auch in das fehlersichere Ausgabegerät verlagerbar, so daß hier eine besonders schnelle und effektive Verarbeitung und Auswertung der logischen Verknüpfungen möglich ist.

Wenn für das fehlersichere Datenausgabegerät die Verarbeitungseinheit ferner oder alternativ die zeitliche Abfolge der mit dem Nutzinformation übermittelten Prozeßdaten überwacht, und dem mindestens Ausgabekanal nur dann ansteuert, wenn die zeitliche Abfolge der zur Ansteuerung des Ausgabekanals erforderlichen Daten innerhalb vorgebbarer Toleranzen liegt, ist ein sog. Muting möglich, das zur Erhöhung der Sicherheit des automatisierten Prozesses beiträgt. Als Beispiel sei die Absicherung einer Fahrbühne mittels eines induktiven Endschalters und einer Lichtschranke genannt. Die Fahrbühne löst bei ihrer Bewegung sowohl den induktiven Endschalter als auch die Lichtschranke in einer gewissen, durch die Geschwindigkeit der Fahrbühne bestimmten zeitlichen Abfolge aus.

Wenn die zeitliche Abfolge des Eingangs der zugehörigen Signale innerhalb der vorgebenen Toleranzen liegt, kann die Verarbeitung fortgesetzt werden. Eine Person dagegen löst nur die Lichtschranke aus, während das zusätzliche Signal des induktiven Endschalters während der vorgegebenen Toleranzzeit ausbleibt. Eine solche Konstellation ist als Alarmkonstella-

tion auswertbar, auf die mit einer Not-Aus-Behandlung reagiert werden kann.

Wenn für das fehlersichere Datenausgabegerät eine als watchdog ausgebildete und die Verarbeitungseinheit überwachende Überwachungsschaltung vorgesehen ist, welche den mindestens einen Ausgabekanal in einen sicheren Zustand überführt, sobald eine Fehlfunktion der Verarbeitungseinheit festgestellt ist, ist über die als watchdog ausgebildete Überwachungsschaltung ein zweiter Abschaltweg etabliert. Wenn z.B. die Verarbeitungseinheit nicht mehr in der Lage ist, einen speziellen Ausgang abzuschalten, würde ohne die Überwachungsschaltung ein Motor oder ein Aggregat z.B. permanent aktiviert bleiben. Die als watchdog ausgebildete Überwachungsschaltung erkennt derartige Zustände und schaltet beim Erkennen eines solchen Zustands die Ausgänge in einen sicheren Zustand.

Wenn bei dem fehlersicheren Datenausgabegerät, der durch die Verarbeitungseinheit ansteuerbare Ausgabekanal als rücklesbarer Ausgabekanal ausgebildet ist, das dem Ausgabekanal zuführbare Signal auch der Überwachungsschaltung zuführbar ist, die Überwachungsschaltung das ihr zugeführte und das vom Ausgabekanal zurückgelesene Signal vergleicht und bei Abweichungen den betroffenen Ausgabekanal oder auch sämtliche Ausgabekanäle bzw. die daran angeschlossene Peripherie in einen sicheren Zustand überführt, werden Diskrepanzen der Ansteuerung der jeweiligen Ausgabekanäle erkannt und diese unmittelbar in einen sicheren Zustand überführt.

Weitere Merkmale, Vorteile und Anwendungsmöglichkeiten der vorliegenden Erfindung ergeben sich aus den Unteransprüchen der nachfolgenden Beschreibung von Ausführungsbeispielen anhand der Zeichnung und der Zeichnung selbst. Dabei bilden alle beschriebenen und/oder bildlich dargestellten Merkmale für

sich oder in beliebiger Kombination den Gegenstand der vorliegenden Erfindung, unabhängig von ihrer Zusammenfassung in den Patentansprüchen oder deren Rückbeziehung. Dabei zeigen:

FIG 1 ein vereinfachtes Blockschaltbild eines Automatisierungssystem,

FIG 2 ein Blockschaltbild eines fehlersicheren Dateneingabegerätes und

FIG 3 ein Blockschaltbild eines fehlersicheren Datenausgabegerätes.

In FIG 1 ist exemplarisch ein Blockschaltbild eines einfachen Automatisierungssystemes mit einem fehlersicheren Dateneingabegerät 2, einem fehlersicheren Datenausgabegerät 3, und einem übergeordneten Automatisierungsgerät 1, z.B. der Zentraleinheit 1 einer speicherprogrammierbaren Steuerung dargestellt. Die Geräte sind über einen Bus 4, vorzugsweise über einen zum Einsatz in Industrieumgebungen geeigneten Bus 4, insbesondere den Profibus 4, kommunikativ miteinander verbunden.

An das fehlersichere Dateneingabegerät 2 ist ein Not-Aus-Taster 1' angeschlossen. An das fehlersichere Datenausgabegerät 3 ist ein Motor 2' angeschlossen. Wenn der Not-Aus-Taster 1' betätigt wird, nimmt das Dateneingabegerät 2 dieses Signal auf, übermittelt es über den Bus 4 an das Datenausgabegerät 3, der daraufhin das Abschalten des Motors 2' bewirkt.

In FIG 2 ein Blockschaltbild ist einer ersten Ausgestaltung eines fehlersicheren Dateneingabegerätes 2 dargestellt. Das fehlersichere Dateneingabegerät 2 ist über den Bus 4 kommunikativ mit anderen an den Bus 4 angeschlossenen Geräten 1, 2, 3, verbunden, dabei ist die Busanschaltung durch ein Bus-

ASICs 5 bewirkt. Die Funktionen des Datenausgabegerätes 3 werden durch eine Verarbeitungseinheit 6, die z.B. ein ASIC oder einen Mikroprozessor ist, bewirkt. Der Verarbeitungseinheit 6 werden direkt oder indirekt die Eingangskanäle 7-0, 7-1...7-7 zugeführt.

Ferner ist im Dateneingabegerät 2 eine Prüfschaltung 8 vorgesehen, die gleichfalls durch die Verarbeitungseinheit 6 kontrolliert wird und zu vorgegebenen Zeitpunkten einen Prüfvorgang auslöst und dabei für mindestens einen der Eingabekanäle 7-0, 7-1...7-7 des fehlersicheren Dateneingabegeräts 2 einen Statuswechsel bewirkt. Dieser Statuswechsel wird von einer internen Logik 9 überwacht, wobei die interne Logik 9 eine Fehlermeldung ausgibt, wenn der von der Prüfschaltung 8 ausgelöste Statuswechsel sich nicht auf den Status des jeweiligen Eingangskanal 7-0, 7-1...7-7 auswirkt. Am Ende des Prüfvorgangs wird der durch die Prüfschaltung 8 bewirkte Statuswechsel wieder rückgängig gemacht. Für das Auslesen der betroffenen Eingabekanäle 7-0, 7-1...7-7 während des normalen Betriebs des fehlersicheren Dateneingabegeräts 2 ist der Prüfvorgang dabei vollkommen transparent.

Wenn die Eingänge 7-0, 7-1...7-7 der Verarbeitungseinheit 6 zusätzlich auch in negierter Form 7-0', 7-1'... 7-7' zugeführt werden, sind die Eingangskanäle antivalent ausgelegt. Die Verarbeitungseinheit 6 liest dann für den betreffenden Eingangskanal, z.B. 7-2 dessen Status, z.B. logisch 0, und für den antivalenten korrespondierenden Eingang 7-2' als negierten Status das entsprechende Komplement, in diesem Falle also logisch 1. Fehlfunktionen bei der Weiterleitung der Stati der jeweiligen Eingangskanäle können durch die Verarbeitungseinheit 6 dann einfach und sicher erkannt werden, indem jeweils überprüft wird, ob auf dem jeweiligen Eingangskanal und auf dem dazu antivalenten Eingangskanal komplementäre Stati vorliegen.

In FIG 3 ist ein Blockschaltbild eines fehlersicheren Datenausgabegerätes 3 dargestellt, das mittels eines als Busanschaltung 14 ausgebildeten Bus-ASICs 14 an den Prozeßbus 4 angeschlossen ist. Das fehlersichere Datenausgabegerät 3 weist eine Verarbeitungseinheit 10 zur Verarbeitung benutzerprojektierbarer logischer Verknüpfungen auf, wobei die Verarbeitungseinheit 10 das Nutzinformation TN eines über den Prozeßbus 4 empfangenen Telegramms auswertet, das Nutzinformation TN der benutzerprojektierbaren logischen Verknüpfung unterwirft, und entsprechend dem Ergebnis der logischen Verknüpfung den mindestens einen Ausgabekanal 11-0, 11-1...11-7 ansteuert.

In der Darstellung gemäß FIG 3 weist das fehlersichere Datenausgabegerät 3 eine als watchdog 12 ausgebildete, und die Verarbeitungseinheit 10 überwachende Überwachungsschaltung 12 auf, welche den mindestens einen Ausgabekanal 11-0, 11-1...11-7 in einen sicheren Zustand überführt, sobald eine Fehlfunktion der Verarbeitungseinheit 10 festgestellt ist. Zu diesem Zweck überwacht die Überwachungsschaltung 12 die Funktion der Verarbeitungseinheit 10, wobei im Falle einer Fehlfunktion der Verarbeitungseinheit 10 die Stati der jeweiligen Ausgabekanäle 11-0, 11-1...11-7 durch die Überwachungsschaltung 12 bestimmt werden, wozu eine Treiberschaltung 13 vorgesehen ist, die sowohl von der Verarbeitungseinheit 10 als auch von der Überwachungsschaltung 12 ansteuerbar ist.

Für den Fall einer Fehlfunktion der Verarbeitungseinheit 10, überschreibt die durch die Überwachungsschaltung 12 ausgegebene Ansteuerung der jeweiligen Ausgabekanäle 11-0, 11-1...11-7 die jeweilige Ansteuerung der Verarbeitungseinheit 10, die zu diesem Zeitpunkt bereits als fehlerhaft erkannt wurde.

In der Darstellung gemäß FIG 3 ist das fehlersichere Datenausgabegerät 3 ferner derartig ausgebildet, daß der durch die Verarbeitungseinheit ansteuerbare Ausgabekanal 11-0, 11-1...11-7 als rücklesbarer Ausgabekanal 11-0', 11-1'... 11-7' ausgebildet ist, daß das dem Ausgabekanal 11-0, 11-1...11-7 zuführbare Signal auch der Überwachungsschaltung 12 zuführbar ist, daß die Überwachungsschaltung 12 das ihr zugeführte und das vom Ausgabekanal zurückgelesene Signal 11-0', 11-1'...11-7' vergleicht und bei Abweichungen den betroffenen Ausgabekanal 11-0, 11-1...11-7 in einen sicheren Zustand überführt.

In der vorstehenden Beschreibung wird stets von Eingabe- bzw. Ausgabegeräten 2, 3 mit jeweils acht Eingabe- bzw. Ausgabekanälen ausgegangen. Selbstverständlich kann die Anzahl der Kanäle auch größer oder kleiner als acht, z.B. 16 oder 32, sein.

Patentansprüche

1. Verfahren zum Betrieb eines Automatisierungssystems,
- wobei das Automatisierungssystem mindestens eine Eingabeeinheit zur Aufnahme von Prozeßsignalen und mindestens eine Ausgabeeinheit zum Ansteuern externer Peripherie aufweist, die kommunikativ über einen Bus miteinander verbunden sind, dadurch gekennzeichnet,
- daß zumindest eine der Eingabeeinheiten und zumindest eine der Ausgabeeinheiten als fehlersichere Eingabeeinheit (EE) bzw. fehlersichere Ausgabeeinheit (AE) ausgebildet sind,
- daß die fehlersichere Eingabeeinheit (EE) der fehlersicheren Ausgabeeinheit (AE) zu vorgegebenen Zeitpunkten ein Telegramm (T) übermittelt,
- daß das Telegramm (T) zumindest ein Nutzinformation (TN), eine die adressierte Ausgabeeinheit (AE) bezeichnende Zielkennung (TT) und eine die sendende Eingabeeinheit (EE) bezeichnende Ursprungskennung (TS) aufweist,
- daß die Ausgabeeinheit (AE) den kontinuierlichen Empfang des Telegramms (T) als Indiz für eine intakte Kommunikationsbeziehung auswertet und andernfalls die angeschlossene Peripherie in einen sicheren Zustand überführt.

2. Fehlersicheres Dateneingabegerät mit mindestens einem Eingabekanal zum Anschluß peripherer Sensorik zur Anwendung in einem Verfahren zum Betrieb eines Automatisierungssystems nach Anspruch 1, dadurch gekennzeichnet, daß eine Prüfschaltung vorgesehen ist, die zu vorgegebenen Zeitpunkten einen Prüfvorgang auslöst und dabei für mindestens einen der Eingabekanäle des fehlersicheren Dateneingabegerätes einen Statuswechsel bewirkt, wobei eine interne Logik den Statuswechsel überwacht und gegebenenfalls eine Fehlermeldung ausgibt, wobei der durch die Prüfschaltung bewirkte Statuswechsel am Ende des Prüfvorgangs wieder rückgän-

gig gemacht wird und wobei der Prüfvorgang für das Auslesen des betroffenen Eingabekanals vollkommen transprarent ist.

3. Fehlersicheres Dateneingabegerät mit mindestens einem Eingabekanal zum Anschluß peripherer Sensorik zur Anwendung in einem Verfahren zum Betrieb eines Automatisierungssystems nach Anspruch 1, dadurch gekennzeichnet, daß der mindestens eine Eingabekanal antivalent ausgelegt ist.

4. Fehlersicheres Datenausgabegerät mit mindestens einem Ausgabekanal zum Anschluß peripherer Aktorik zur Anwendung in einem Verfahren zum Betrieb eines Automatisierungssystems nach Anspruch 1, dadurch gekennzeichnet, daß eine Verarbeitungseinheit zur Verarbeitung benutzerprojektierbarer logischer Verknüpfungen vorgesehen ist, wobei die Verarbeitungseinheit das Nutzinformation (TN) eines empfangenen Telegramms (T) auswertet, das Nutzinformation der benutzerprojektierbaren logischen Verknüpfung unterwirft und ensprechend dem Ergebnis der logischen Verknüpfung den mindestens einen Ausgabekanal ansteuert.

5. Fehlersicheres Datenausgabegerät nach Anspruch 4, dadurch gekennzeichnet, daß die Verarbeitungseinheit die zeitliche Abfolge der mit dem Nutzinformation (TN) übermittelten Prozeßdaten überwacht und den mindestens einen Ausgabekanal nur dann ansteuert, wenn die zeitliche Abfolge der zur Ansteuerung der Ausgabekanals erforderlichen Daten innerhalb vorgegebener Toleranzen liegt.

6. Fehlersicheres Datenausgabegerät nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß eine als Watchdog ausgebildete und die Verarbeitungseinheit überwachende Überwachungsschaltung vorgesehen ist, welche den mindestens einen Ausgabekanal in einen sicheren Zustand über-

führt, sobald eine Fehlfunktion der Verarbeitungseinheit festgestellt ist.

7. Fehlersicheres Datenausgabegerät nach Anspruch 6, d a - d u r c h g e k e n n z e i c h n e t , daß der durch die Verarbeitungseinheit ansteuerbare Ausgabekanal als rücklesbarer Ausgabekanal ausgebildet ist, daß das dem Ausgabekanal zuführbare Signal auch der Überwachungsschaltung zuführbar ist, daß die Überwachungsschaltung das ihr zugeführte und das vom Ausgabekanal zurückgelesene Signal vergleicht und bei Abweichungen den betroffenen Ausgabekanal oder sämtliche Ausgabekanäle in einen sicheren Zustand überführt.

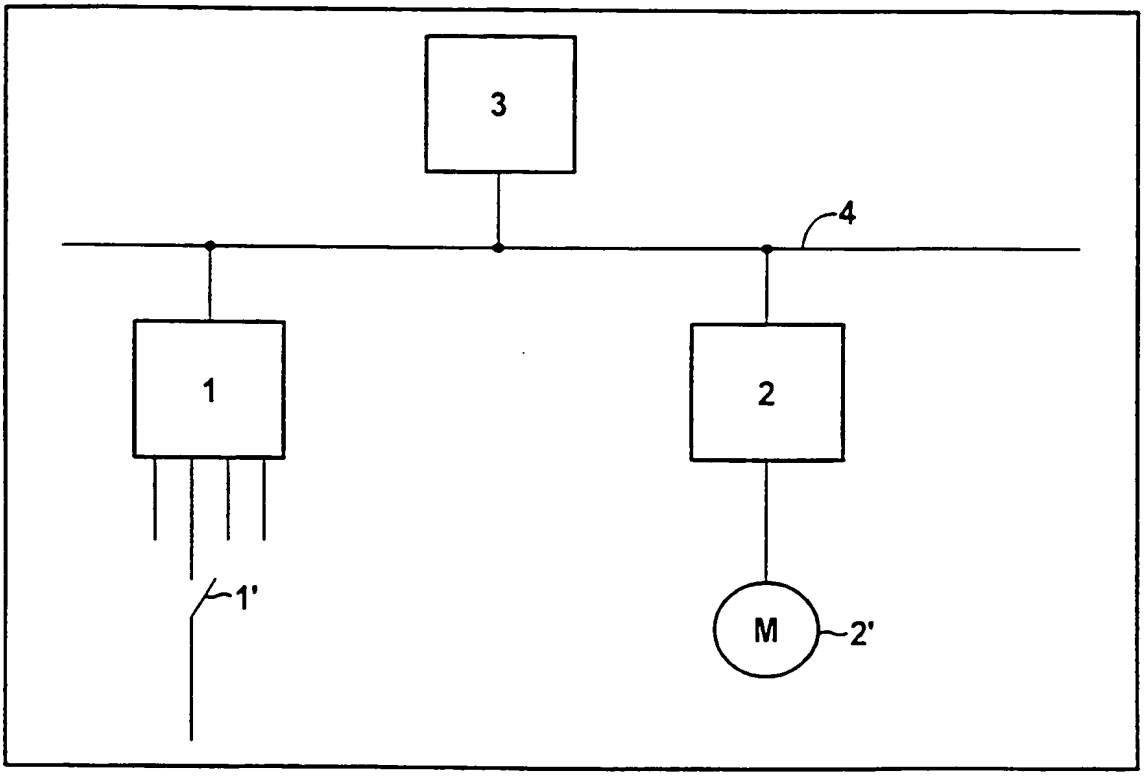


FIG 1

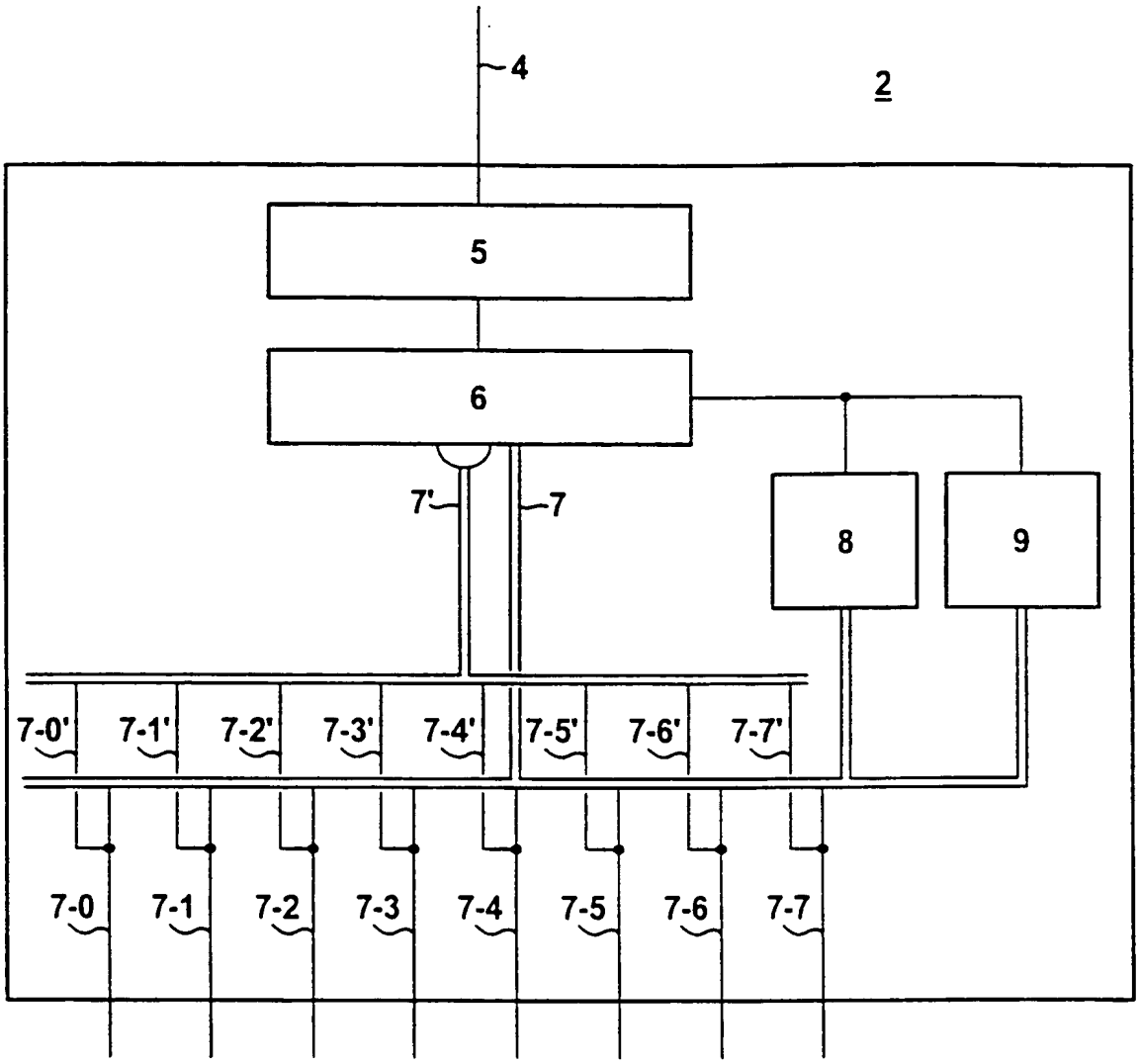


FIG 2

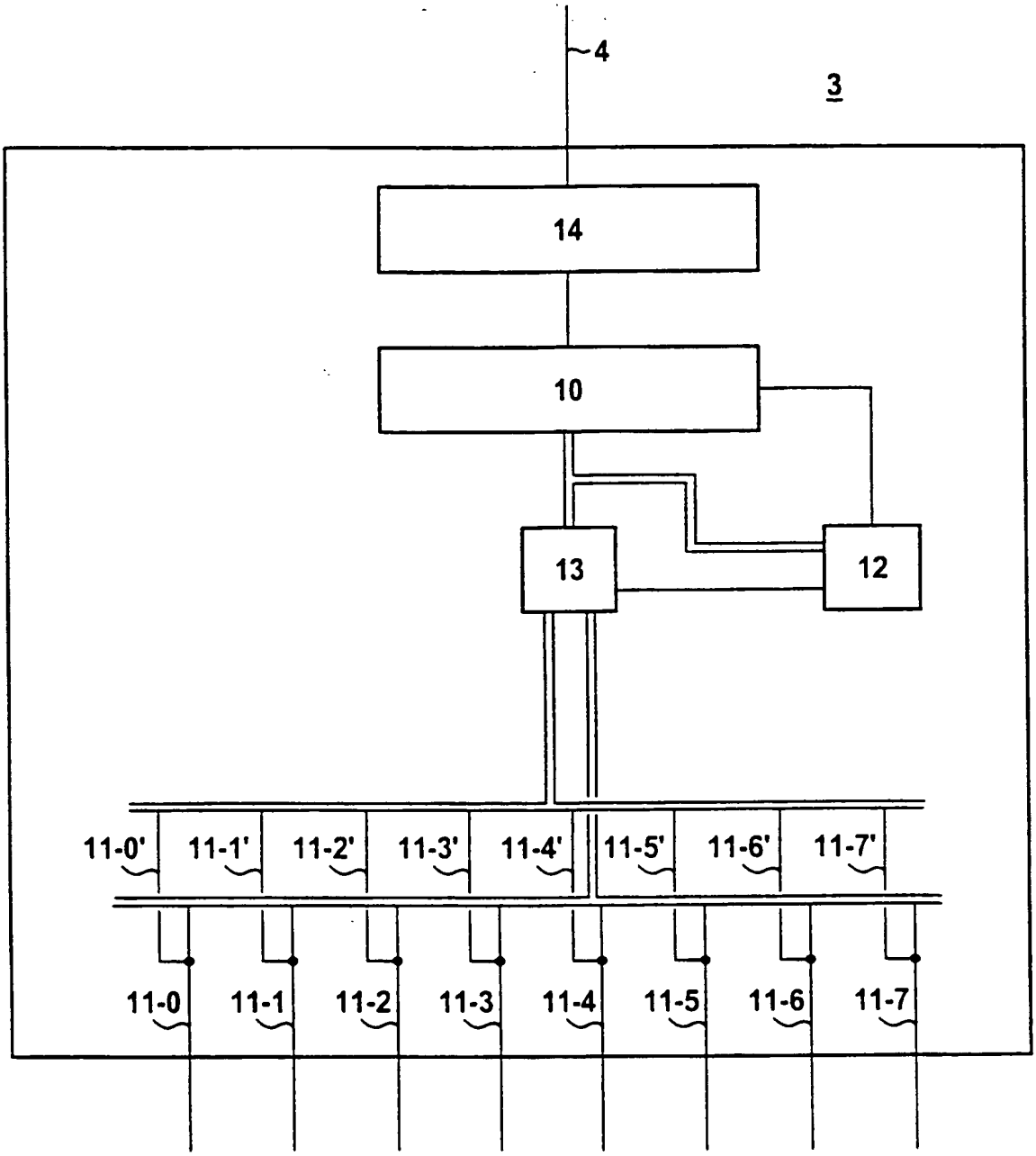

4
3
14
10
13
12
11-0'
11-1'
11-2'
11-3'
11-4'
11-5'
11-6'
11-7'
11-0
11-1
11-2
11-3
11-4
11-5
11-6
11-7

FIG 3

INTERNATIONAL SEARCH REPORT

Int. ational Application No
PCT/DE 98/03771

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G05B19/042 G06F11/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G05B G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 43 12 305 A (ABB PATENT GMBH) 27 October 1994 see column 2, line 31 - column 3, line 21; figure 1	1,2,4-6
X Y	US 4 680 753 A (FULTON TEMPLE L ET AL) 14 July 1987 see column 4, line 41 - column 11, line 51; figures 1-12	1,2,4-7 3
Y	DE 30 24 370 A (SIEMENS AG) 28 January 1982 see page 4, line 33 - page 6, column 12; figures 1,2	3

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 May 1999	18/05/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Tran-Tien, T

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 98/03771

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X,P	EP 0 837 394 A (ELAN SCHALTELEMENTE GMBH) 22 April 1998 see column 6, line 43 - column 11, line 56; figures 1-3	1,2,4-7
A	EP 0 770 942 A (ELAN SCHALTELEMENTE GMBH) 2 May 1997 see column 6, line 7 - column 8, line 30; figures 1,2	1-7
A	EP 0 524 330 B (SIEMENS AG) 30 November 1994 see page 1, line 56 - page 5, line 11; figures 1,2	1-7
A	DE 40 41 550 A (ELAN SCHALTELEMENTE GMBH) 25 June 1992 see column 4, line 43 - column 6, line 60; figures 1,2,5	1-7
A	MOHLENBEIN H: "INTERBUS-DEZENTRALE ECHTZEIT-PERIPHERIE FUER STANDARD-SPS-SYSTEME" ELEKTRIE, vol. 44, no. 7, 1 January 1990, pages 244-249, XP000162759 see paragraph 4-8	1-7
A	HERTEL J: "ABSOLUT SICHERES GELEIT. REDUNDANZSTRUKTUREN IM MODERNEN PROZESSLEITSYSTEM TELEPERM XP" MESSEN UND PRUFEN, vol. 31, no. 10, 1 October 1995, pages 10, 12-14, 16, XP000543694 see the whole document	1-7

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Im ..tional Application No
PCT/DE 98/03771

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 4312305 A	27-10-1994	NONE	
US 4680753 A	14-07-1987	DE 3689052 D	28-10-1993
		DE 3689052 T	13-01-1994
		EP 0200365 A	05-11-1986
		JP 1894678 C	26-12-1994
		JP 6024371 B	30-03-1994
		JP 61257039 A	14-11-1986
DE 3024370 A	28-01-1982	AT 385364 B	25-03-1988
		CH 654425 A	14-02-1986
EP 0837394 A	22-04-1998	DE 19643092 A	30-04-1998
		JP 10228426 A	25-08-1998
EP 0770942 A	02-05-1997	DE 19540069 A	30-04-1997
EP 0524330 B	27-01-1993	EP 0524330 A	27-01-1993
		AT 114835 T	15-12-1994
		DE 59103707 D	12-01-1995
		JP 5225481 A	03-09-1993
		US 5394409 A	28-02-1995
DE 4041550 A	25-06-1992	NONE	

INTERNATIONALER RECHERCHENBERICHT

In. ationales Aktenzeichen
PCT/DE 98/03771

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G05B19/042 G06F11/00

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G05B G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 43 12 305 A (ABB PATENT GMBH) 27. Oktober 1994 siehe Spalte 2, Zeile 31 - Spalte 3, Zeile 21; Abbildung 1 ---	1,2,4-6
X Y	US 4 680 753 A (FULTON TEMPLE L ET AL) 14. Juli 1987 siehe Spalte 4, Zeile 41 - Spalte 11, Zeile 51; Abbildungen 1-12 ---	1,2,4-7 3
Y	DE 30 24 370 A (SIEMENS AG) 28. Januar 1982 siehe Seite 4, Zeile 33 - Seite 6, Spalte 12; Abbildungen 1,2 --- -/--	3

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
5. Mai 1999	18/05/1999
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	**Bevollmächtigter Bediensteter** Tran-Tien, T

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

In: ...tionales Aktenzeichen
PCT/DE 98/03771

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X,P	EP 0 837 394 A (ELAN SCHALTELEMENTE GMBH) 22. April 1998 siehe Spalte 6, Zeile 43 - Spalte 11, Zeile 56; Abbildungen 1-3	1,2,4-7
A	EP 0 770 942 A (ELAN SCHALTELEMENTE GMBH) 2. Mai 1997 siehe Spalte 6, Zeile 7 - Spalte 8, Zeile 30; Abbildungen 1,2	1-7
A	EP 0 524 330 B (SIEMENS AG) 30. November 1994 siehe Seite 1, Zeile 56 - Seite 5, Zeile 11; Abbildungen 1,2	1-7
A	DE 40 41 550 A (ELAN SCHALTELEMENTE GMBH) 25. Juni 1992 siehe Spalte 4, Zeile 43 - Spalte 6, Zeile 60; Abbildungen 1,2,5	1-7
A	MOHLENBEIN H: "INTERBUS-DEZENTRALE ECHTZEIT-PERIPHERIE FUER STANDARD-SPS-SYSTEME" ELEKTRIE, Bd. 44, Nr. 7, 1. Januar 1990, Seiten 244-249, XP000162759 siehe Absatz 4-8	1-7
A	HERTEL J: "ABSOLUT SICHERES GELEIT. REDUNDANZSTRUKTUREN IM MODERNEN PROZESSLEITSYSTEM TELEPERM XP" MESSEN UND PRUFEN, Bd. 31, Nr. 10, 1. Oktober 1995, Seiten 10, 12-14, 16, XP000543694 siehe das ganze Dokument	1-7

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

In ...tionales Aktenzeichen
PCT/DE 98/03771

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
DE 4312305	A	27-10-1994	KEINE		
US 4680753	A	14-07-1987	DE	3689052 D	28-10-1993
			DE	3689052 T	13-01-1994
			EP	0200365 A	05-11-1986
			JP	1894678 C	26-12-1994
			JP	6024371 B	30-03-1994
			JP	61257039 A	14-11-1986
DE 3024370	A	28-01-1982	AT	385364 B	25-03-1988
			CH	654425 A	14-02-1986
EP 0837394	A	22-04-1998	DE	19643092 A	30-04-1998
			JP	10228426 A	25-08-1998
EP 0770942	A	02-05-1997	DE	19540069 A	30-04-1997
EP 0524330	B	27-01-1993	EP	0524330 A	27-01-1993
			AT	114835 T	15-12-1994
			DE	59103707 D	12-01-1995
			JP	5225481 A	03-09-1993
			US	5394409 A	28-02-1995
DE 4041550	A	25-06-1992	KEINE		